AMENDMENTS TO THE CLAIMS:

1. (Currently Amended) A method of detecting computer viruses, comprising:

providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ~~and~~

an antivirus unit ,that uses a particular operating system, scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned by the antivirus unit includes at least some parts of the first and second segments; and

the antivirus unit accessing non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses.

2. (Original) A method, according to claim 1, wherein said first and second segments correspond to different physical portions of the disk space.

3. (Original) A method, according to claim 2, wherein said first and second segments overlap.

4. (Original) A method, according to claim 2, wherein the first and second segments do not overlap.

5. (Original) A method, according to claim 1, wherein the first and second segments correspond to logical entities.

6. (Original) A method, according to claim 5, wherein said first and second segments overlap.

7. (Original) A method, according to claim 5, wherein the first and second segments do not overlap.

8. (Original) A method, according to claim 1, wherein the first and second segments correspond to logical entities.

9. (Original) A method, according to claim 1, wherein the part of the disk space that is scanned by the antivirus unit corresponds to files that have been modified since a previous virus scan.

10. (Original) A method, according to claim 9, further comprising:

examining a date of last modification for each of the files; and

determining which files have been modified since a previous virus scan using the date of last modification for each of the files.

11. (Original) A method, according to claim 10, further comprising:

in response to a date of last modification indicating a file has been modified since a previous virus scan, scanning the file for viruses.

12. (Original) A method, according to claim 11, further comprising:

in response to date information indicating that a file has not been modified since a previous virus scan, comparing a current size of the file with a previous size of the file determined during the previous virus scan; and

in response to the current size being different from the previous size, rescanning the file.

13. (Original) A method, according to claim 1, further comprising:

implementing at least part of the antivirus unit using stand alone hardware.

14. (Original) A method, according to claim 1, further comprising:

implementing at least part of the antivirus unit as a process running on at least one of the hosts.

15. (Original) A method, according to claim 1, wherein useable areas of the disk space are partitioned into separate segments.

16. (Original) A method, according to claim 1, wherein the antivirus unit scans useable areas of the disk space.

17. (Original) A method, according to claim 1, wherein the antivirus unit scans at least part of the disk space independently of any file structures corresponding to the disk space.

18. (Original) A method, according to claim 1, wherein a particular segment assigned to a first host is inaccessible to other hosts.

19. (Original) A method, according to claim 18, wherein all of the segments are at least readable by the antivirus unit.

20. (Original) A method, according to claim 1, wherein at least a portion of the antivirus unit is provided on at least some controllers for disks corresponding to the disk space.

21. (Original) A method, according to claim 20, wherein the antivirus unit is provided with file structure information for files stored in the disk space.

22. (Currently Amended) A method of scanning a storage device for viruses, comprising:

performing a first virus scan at a first time; and

performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system.

23. (Original) A method, according to claim 22, wherein performing the second virus scan includes scanning only entities having one of a predetermined set of types.

24. (Original) A method, according to claim 22, wherein performing the second virus scan includes:

for each of the logical entities having a date of last modification that is prior to the first time, comparing a current size value of the entity with a previous size value of the entity prior to the most previous virus scan; and

scanning entities having at least one of: a date of last modification that is after the first time and the current size value that is different than the previous size value.

25. (Original) A method, according to claim 22, wherein performing the second virus scan includes:

for each of the logical entities having one of a predetermined set of types and having a date of last modification that is prior to the first time, comparing a current size value of the entity with a previous size value of the entity prior to the first time; and

scanning entities having one of the predetermined set of types and having at least one of: a date of last modification that is after the first time and the current size value that is different than the previous size value.

26. (Currently Amended) A computer program product for detecting computer viruses, comprising:

means for accessing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ~~and~~

means that uses a particular operating system for scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned includes at least some parts of the first and second segments; and

means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses.

27. (Original) A computer program product, according to claim 26, wherein said first and second segments correspond to different physical portions of the disk space.

28. (Original) A computer program product, according to claim 27, wherein said first and second segments overlap.

29. (Original) A computer program product, according to claim 27, wherein the first and second segments do not overlap.

30. (Original) A computer program product, according to claim 26, wherein the first and second segments correspond to logical entities.

31. (Original) A computer program product, according to claim 26, wherein the part of the disk space that is scanned by the antivirus unit corresponds to particular types of files stored in the disk space.

32. (Original) A computer program product, according to claim 26, wherein the part of the disk space that is scanned by the antivirus unit corresponds to files that have been modified since a previous virus scan.

33. (Original) A computer program product, according to claim 32, further comprising:

means for examining a date of last modification for each of the files; and

means for determining which files have been modified since a previous virus scan using the date of last modification for each of the files.

34. (Original) A computer program product, according to claim 33, further comprising:

means for scanning the file for viruses in response to a date of last modification indicating a file has been modified since a previous virus scan.

35. (Original) A computer program product, according to claim 34, further comprising:

means for comparing a current size of the file with a previous size of the file determined during the previous virus scan in response to date information indicating that a file has not been modified since a previous virus scan; and

means for rescanning the file in response to the current size being different from the previous size.

36. (Currently Amended) A computer program product for scanning a storage device for viruses, comprising:

means for performing a first virus scan at a first time; and

means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after ~~to~~ the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system.

37. (Original) A computer program product, according to claim 36, wherein said means for performing the second virus scan scans entities having one of a predetermined set of types.

38. (Original) A computer program product, according to claim 36, wherein said means for performing the second virus scan compares a current size value of the entity with a previous size value of the entity prior to the most previous virus scan for each of the logical entities having a date of last modification that is prior to the first time and scans entities having at least one of: a date of last modification that is after the first time and the current size value that is different than the previous size value.

39. (Currently Amended) An antivirus scanning unit, comprising:

means for coupling to at least one storage device having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; ~~and~~

means for using a particular operating system for scanning at least part of the at least one storage device for viruses, wherein the part that is scanned includes at least some parts of the first and second segments; and

means for accessing non-native files created using operating systems different from the particular operating system that is used in connection with scanning at least parts of the disk space for viruses.

40. (Original) An antivirus unit, according to claim 39, wherein said means for coupling includes means for coupling to only one storage device.

41. (Original) An antivirus unit, according to claim 39, wherein said means for coupling includes means for coupling to more than one storage device.

42. (Original) An antivirus unit, according to claim 39, further comprising:

means for coupling to at least one host.

43. (Original) An antivirus unit, according to claim 42, wherein said antivirus unit is interposed between said at least one storage device and said at least one host.

44. (Original) An antivirus unit, according to claim 42, wherein said antivirus unit is implemented as a process running on the at least one host.

45. (Original) An antivirus unit, according to claim 39, wherein said antivirus unit is implemented using stand alone hardware.

46. (Original) An antivirus unit, according to claim 39, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

47. (Currently Amended) An antivirus unit, comprising:

means for performing a first virus scan at a first time; and

means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system.

48. (Original) An antivirus unit, according to claim 47, wherein said means for performing the second virus scan scans only entities having one of a predetermined set of types.

49. (Original) An antivirus unit, according to claim 47, wherein said antivirus unit is implemented using stand alone hardware.

50. (Original) An antivirus unit, according to claim 47, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.